2012 NASCIO RECOGNITION AWARD NOMINATION

Integrating Cyber and Physical Security: Ending the Divide Using a Comprehensive Approach to Risk

Nomination Category:
Cyber Security Initiatives

Name of State Agency:
State of Michigan
Department of Technology, Management & Budget (DTMB)

Project Manager:
Dan Lohrmann, Chief Security Officer
(517) 241-4090
Lohrmannd@michigan.gov

Name of Project Executive Sponsors:
David Behen, State CIO
John Nixon, Director DTMB and State Budget Director
Michigan Governor Rick Snyder


DHS Secretary Napolitano


Industry Expert Panel

Michigan Governor Rick Snyder

Section 2 - Executive Summary: After over a decade since September 11, 2001, are we safer or connecting the dots any better? As our physical and virtual worlds merge, technologies to streamline access to information have created new challenges to ensure trust is efficiently maintained across domains. Recent cyber threats, global security trends and coordinated attacks against critical infrastructure have accelerated the need for action and the availability of new solutions, including partnered governance, management and operational designs in order to protect citizens. *Michigan has ended the divide between physical and cybersecurity by establishing an enterprise-wide Chief Security Officer (CSO) and supporting processes. This function reports to the Chief Information Officer (CIO) to identify and manage the full range of threats facing the state and taking appropriate steps to mitigate those risks and thwart attacks.*

Problem Statement: For security to be effective it must be organized to react quickly and communicate effectively to resolve issues across the enterprise. New cyber-attacks, malware, insider threats and other security challenges threaten to derail new innovative government strategies. Identity management and the provisioning of services is more complex at a time when the amount of electronic health records is exploding and identity theft is rampant. A key question is how can governments modernize systems, reduce risk, and protect critical infrastructures at the same time?

Solution: The creation of a new Cybersecurity and Infrastructure Protection (CIP) organization addresses numerous issues while reducing redundancy and maximizing security coordination. This solution also includes: the launch of the Michigan Cyber Initiative, new cyber training toolkits for government employees, students, schools, and businesses, a new enterprise cyber roadmap, identity management focus combining both physical and virtual (network) access, integrated teams for comprehensive emergency management for physical and cyber incidents, and a combined platform for surveillance management statewide leading to thousands of cameras in an integrated system. This project was highlighted at the Michigan Cyber Summit which was the national kickoff for Cybersecurity Awareness Month in October 2011 with Secretary Napolitano and Howard Schmidt speaking with Governor Rick Snyder.

Significance: Michigan is the first state to merge physical and cybersecurity on an enterprise-wide basis. This model reduces risk and delivers better security with fewer resources by eliminating overlapping duties. Specifically, this approach offers greater executive visibility, creates operational efficiencies, improves risk management, provides streamlined incident management if breaches occur, maximizes existing investments and reduces operational costs. New metrics, processes and procedures have been established across multiple agencies and domains to better coordinate and communicate activities. Our model offers tiers that are easily adaptable to other states.

Benefits: The program has achieved significant improvements in governance, procedures, operations and risk management outcomes:

- Hard savings of at least $500,000 on emergency management staffing functions.
- Improved regulatory compliance (such as PCI) through covering security gaps.
- Streamlined, coordinated response to breaches and security events and exercises.
- Integrated risk management, loss prevention, fraud prevention, business continuity planning strategies. Partnerships enhanced with local and national organizations.

Section 3 - **Business Problem & Solution Description:** In response to an unprecedented increase in security threats and in order to maximize overall technology efficiency and effectiveness, the Michigan Department of Technology Management & Budget (DTMB) has ended the divide between the enterprise-wide physical and cybersecurity organizations with a newly appointed Chief Security Officer (CSO) and Deputy Director for Cybersecurity and Infrastructure Protection (CIP). This project, along with the development of a cybersecurity action plan, strategic security roadmap and surveillance integration sub-project, brought together disparate security functions and created a new entity to enable further technology innovation using a comprehensive, metrics-based approach to reducing physical and cyber risks.

Problem Background: When Governor Rick Snyder first took office in January 2011, he immediately emphasized the strategic importance of enabling citizens and reinventing government through the use of smart technology and further enabling innovations such as mobile computing, cloud computing, data analytics and business process reengineering. With a background as CEO of Gateway Computers, the Governor also stressed that measuring cyber risks and creating cyber business opportunities needed to be top priorities. This meant implementing a new approach to converged security, following models in the leading private sector organizations around the world.

This new executive management team was briefed about attacks via the Internet that Michigan faces every day (see metrics provided in early 2011 that precipitated this project.) The federal government also predicted new cyber-attacks were coming.

Facts on Cyber Attacks presented to new leadership in January 2011

- 2010 State of Michigan
  - 29,942 Blocked Web browser attacks
  - 24,671 Blocked Web Site attacks
  - 14,072 Blocked Network Scans
  - 88,774 Blocked Intrusion attempts

- 2010 National Statistics
  - 79.9% of websites with malicious code were legitimate sites that have been compromised
  - 89.9% of all unwanted emails in circulation during this period contained links to spam sites or malicious websites
  - Data theft and breaches from cyber-crime may cost businesses as much as $1 trillion globally

Facing new cyber as well as physical security threats, the need for a holistic view of the security function was recognized. A cross-sector team was assembled in the spring of 2011 which included state, local and federal government experts, private sector companies, P-20 education, universities and others. Within state government, representatives from criminal justice agencies, including lawyers, functional leads and human resource staff, all participated in a comprehensive look at what was needed to address the cyber and infrastructure protection challenges.

Scope of Problem: Assembled experts identified the need to offer solutions to protect the overall security ecosystem and to enable economic development for cybersecurity. Security threats were seen as both problems and opportunities. Actions were needed

around three distinct but equally important pillars: confidentiality, integrity and availability (see chart below). Outcomes affect home users, small business, communities, large commercial enterprises, and critical infrastructure. In addition, the need for new governance, risk assessment, defined budget, and an implementation plan starting with access controls, was clear.

Principal drivers of integrated security include: common access cards, video surveillance, improved emergency management training, joint exercises, situational response, business continuity and data center security. Industry experts advised us that as long as organizations treat their physical and cyber domains as separate, there is little hope of securing either one.

New partnerships were needed cutting across public/private sectors as well as federal/ state/local governments and various education groups. Improving our coordinated response across critical infrastructure areas was identified as top action item along with new awareness training. Issues were grouped into people / process / technology areas.

Ecosystem Component	Confidentiality	Integrity	Availability
Homes, Individuals, Small Business & Schools	Confidential medical records should be released only to those people or organizations (i.e., doctor, hospital, insurance, government agency, etc.) authorized to review them.	The records should be well protected so that no one can change the information without authorization.	The records should be available and accessible to authorized users.
Large Industry, Government Agencies, Commercial, & Academic Institutions	Technical documents regarding a research and development program for an innovative mechanical device must be safeguarded from theft by competitors or industrial espionage.	The technical specifications for a novel device must be protected from manipulation.	The information must be able to be shared with appropriate divisions within the company and with the government agency sponsoring the program.
Infrastructures (e.g., Utility Providers, Banking & Financial, & Transportation)	Information about financial accounts at a local bank must not be made available to anyone without the account owner's expressed authorization.	The databases pertaining to various accounts for home and auto loans, investments, etc., must be safeguarded by financial institutions from tampering or data being divulged to unauthorized parties.	The information concerning savings, checking, loan and investment balances must be readily available to the account owner using appropriate ID and password via online systems.

Solution Description:

Phase I: ***Basic Management Integration*** – After detailed planning and reorganization sessions were held, the Cybersecurity & Infrastructure Protection (CIP) organization

was formally operational on October 1, 2011. This project included over sixty state staff and 400 contractors coming together with physical security and cybersecurity directors reassigned to report to the new Chief Security Officer. This effort was an additional step following the merger of the Michigan Department of Information Technology (MDIT) and the Department of Management & Budget (DMB) to form the Department of Technology, Management & Budget (DTMB). This group worked quickly to build the action plan called the Michigan Cyber Initiative.

Phase II: ***Mid-range, operational IT/Physical integration*** – This step brought together the people, equipment and facility integration from both the cyber and physical security teams. These steps began earlier in 2010 with the establishment of DTMB, and have resulted in newly-integrated identity management, technology integration into smart buildings, video integration and other benefits. The use of Information Technology Infrastructure Library (ITIL) was documented in last year's NASCIO submission, and these concepts were extended into new boundaries such as camera integration across all areas of state government. Functions were examined for the best groupings.

Phase III: ***Full scope-including strategic cyber-infrastructure, public capital investments, critical infrastructure protection, national /local partnerships.***
Michigan began an aggressive journey to completely reinvent how security works. The launch, detailed strategy, detailed project plans, improved logging and ID management were all completed before December 1, 2011 (Parts A, B & C). Other strategies such as securing the smart grid, strengthening health IT, modernizing public safety communications and intelligent transportation are ongoing efforts. The specific actions achieved under these phases are listed in section 4 below.

Section 4 – Significance to Improving Government Operations: This project has immense significance to the operations and addressed numerous executive priorities, including CIO risk reduction efforts and people issues. Specifically:

Phase I – Significant Basic Management Integration - CIP organization established:

- A leader in cyber-awareness and citizen safety training;
- A single entity charged with the oversight of risk management and security issues associated with State of Michigan assets, property, systems and networks;
- Improved efficiency within the state's Department of Technology, Management and Budget with significant saving and redeployment of resources;
- A single entity with combined focus on emergency management efforts in both physical and cyber areas. Joint exercises such as CYBERSTORM and NLE.
- Cross training staff across physical and cyber domains on emergency situations.

Phase II – Significant Mid-Range Strategies / Processes / Operations Implemented

- Met Governor's mandate, Federal requirements, and DTMB requirements to incorporate and modernize Disaster Recover (DR) and emergency management into existing processes. With merged teams, this process became more effective.

- Aligned with Federal, CIO and NASCIO priorities, including: budget and cost control; security enhancement tools; cloud computing; consolidation; virtualization, shared services and solutions. Address new compliance requirements for health IT.
- Developed strategies and operational approaches for more effective management of "stealth threats" and the implications of cloud computing to business operations.

Processes:

- Created new opportunities to consolidate operations and share solutions by migrating to a single DR/COG solution under the Executive Branch with other branches of Government and locals poised to leverage the same solution.
- Creation of policy, funding and staffing model and a process for operationalizing the information by clearly identifying systems risk factors/ solutions.

Operations:

- Creation of an online dashboard reflecting security risks to each agency.
- Metrics for improvements and required actions to reduce risk
- A common security "road show" established for agencies to see security risk.
- Connect the dots between physical security and cyber operations threat activities.

Phase III - Specific Significant Full Scope Efforts from this phase included:

A. Greatly improved cyber awareness campaign that is interactive, relevant and fun.
   1 National launch of Cybersecurity Awareness month at sold-out Michigan Cyber Summit 2011 – see: http://events.esd.org/MichiganCyberSummit2011.aspx
   2 New training for ~50K state employees
   3 New cyber awareness toolkit – see: www.Michigan.gov/cybersecurity

B. Detailed Project Plans and Strategies cutting across public / private sectors.
   1 New Statewide Cyber Rapid Response Team for incidents
   2 New Joint Cyber Command Center collocated with Michigan State Police
   3 New Security Operations Center (SOC)

C. Enhanced National Partnerships with FBI, InfraGard, DHS and MS-ISAC.
   1 First State to launch "Albert" Intrusion Detection System with MS-ISAC
   2 Coordination role on DHS Government Coordinating Council for NASCIO (One outcome led to State CIOs being briefed by NSA on threats.)

D. New Michigan Cyber Range in partnership with universities – this public/ private partnership is a test bed for testing global cyber threats and solutions.

E. New card access systems and identity management coordination. Pilots are complete, and massive expansion is underway.

F. Efforts on smart grid, health IT security, new health information network security and strengthening of public safety communications all underway in 2011.

G. Extensive progress toward common video surveillance, business continuity and data center security.

Section 5 - Benefit of the Project: In addition to supporting the security requirements of all state agencies, this center of excellence in best-practice security services offers assistance for Michigan local governments via the MI-ISAC. This organization is responsible for coordinating with national partners such as DHS, FBI and MS-ISAC and other states. Michigan is also helping other states who are considering this approach to

integrating physical and cybersecurity. The program has achieved significant improvements in governance, procedures, operations and risk management outcomes:

Project achieved hard savings of $500,000 on emergency management staffing functions and potentially millions in incident avoidance through improved, integrated security. The average cyber breach costs over $6 million per incident according to The Ponemon Institute. Note: Financial calculations include the eliminated need for five overlapping staffing positions performing emergency management work that cost an average of $100,000 each with salary and benefits. These positions have been merged into one organization – allowing these staff to perform other functions. (We went from 10 staff to 5 in this emergency management and DR area – with better coordination and coordinated results.)

Improved regulatory compliance through covering security gaps.

- Strengthen security in existing (and future) infrastructure, cabling, data networks, wireless and mobile computing projects. See: Michigan Cyber Initiative
- Coordinated response process established for breaches and security events.
- Agency projects completed more securely included: PCI Compliance & IRS audit findings closed (Dept. of Treasury), health information sharing efforts (Dept. of Community Health).

Integrated risk management, loss prevention, fraud prevention, business continuity planning strategies. Security liaison roles redefined.

- New metrics to measure and systematically reduce cyber and physical risk.
- Improved Continuity of Operations (COOP), Continuity of Government (COG), and emergency management coordination. This has played out in power outages, malware attacks, and denial of service attacks against the state.

Improved security training - enhanced existing staffing skillsets in cyber and physical security areas. This has improved morale and overall teamwork of staff.

- Improved end users training – see also: Security Breakfast Roadshow
- Online training and awareness for citizens regarding cyber threats

New architecture for access cards, improved video surveillance, business continuity and data center security.

- Plans completed for Security Operations Center (SOC), Rapid Cyber Defense Response Team (Public/Private), and new Michigan Cyber Command Center
- The development of a comprehensive security strategy (see - Michigan Cyber Initiative) for all Michigan resources and infrastructure (completed and launched on October 2011).

Project responds proactively to **address new global cyber threats** (examples of threats: http://www.washingtonpost.com/zero-day?hpid=z1)

In conclusion, this project is the result of a systematic approach to risk reduction and mitigating security threats - connecting the physical and cyber domains. Gartner, Forrester, and many Fortune 500 companies recommend this approach for mature organizations in order to facilitate efficient security operations and planning. Michigan has taken the next step in implementing effective, holistic enterprise-wide security.